

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

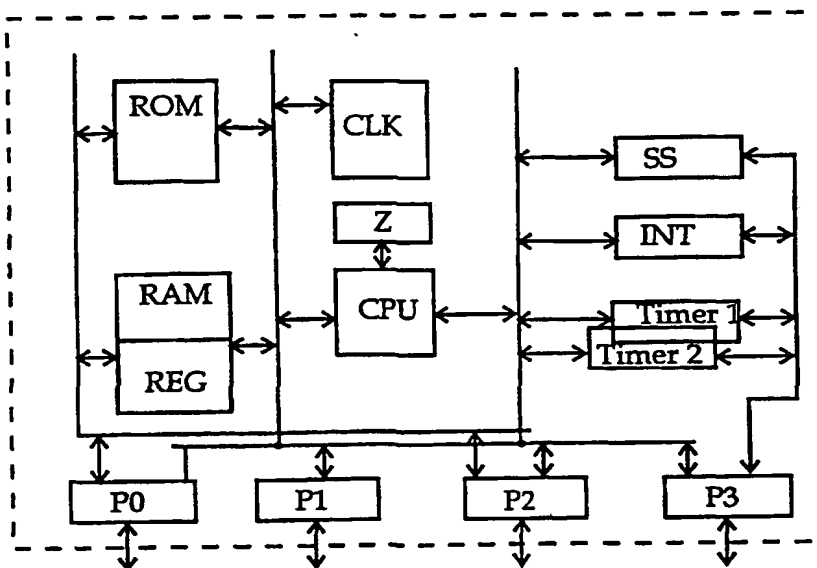
(51) Internationale Patentklassifikation ⁷ : G06F 11/00		A1	(11) Internationale Veröffentlichungsnummer: WO 00/65442
		(43) Internationales Veröffentlichungsdatum:	2. November 2000 (02.11.00)
(21) Internationales Aktenzeichen: PCT/EP00/03530 (22) Internationales Anmeldedatum: 19. April 2000 (19.04.00) (30) Prioritätsdaten: 199 18 620.0 23. April 1999 (23.04.99) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregen- tenstr. 159, D-81677 München (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): BALDISCHWEILER, Michael [DE/DE]; Friedrich-Eckardstr. 60, D-81929 München (DE). (74) Anwalt: KLUNKER, SCHMITT-NILSON, HIRSCH; Winzer- estr. 106, D-80797 München (DE).		(81) Bestimmungsstaaten: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Veröffentlicht Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.	

(54) Title: PROTECTION OF THE CORE PART OF A COMPUTER AGAINST EXTERNAL MANIPULATION

(54) Bezeichnung: SICHERUNG EINES RECHNERKERNS GEGEN ÄUSSERE MANIPULATIONEN

(57) Abstract

The invention relates to a method for protecting the central processing unit of a computer, especially a chip card. After the CPU has processed a command, individual sensitive registers are logically interlinked to produce a checksum. This checksum is stored and compared with an appropriately produced checksum before the next command begins to be processed. If the compared checksums do not match, this indicates that the contents of the register of the CPU have been manipulated during the time between the two commands being processed. In this case, an error message is produced accordingly and the processor is stopped or the card is withdrawn.



(57) Zusammenfassung

Es wird ein Verfahren zur Sicherung der zentralen Verarbeitungseinheit eines Rechners, insbesondere einer Chipkarte, vorgeschlagen. Einzelne sicherheitsrelevante Register werden logisch miteinander verknüpft um eine Checksumme zu bilden, nachdem die CPU einen Befehl abgearbeitet hat. Diese Checksumme wird gespeichert und vor Beginn der Verarbeitung des nächstfolgenden Befehls mit einer entsprechend gebildeten Checksumme verglichen. Stimmen die miteinander verglichenen Checksummen nicht überein, so deutet das auf eine Manipulation der Registerinhalte der CPU im Zeitraum zwischen der Abarbeitung der beiden Befehle hin. In einem solchen Fall ergeht eine entsprechende Fehlermeldung und der Prozessor wird angehalten, oder die Karte wird eingezogen.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland		Republik Mazedonien	TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von
CA	Kanada	IT	Italien	MX	Mexiko		Amerika
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun		Korea	PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Sicherung eines Rechnerkerns gegen äußere Manipulationen

- 5 Die vorliegende Erfindung betrifft die Sicherung eines Rechners gegen äußere Manipulationen, insbesondere die Sicherung der im Rechnerkern bzw. zentralen Verarbeitungseinheit (CPU) vorliegenden Daten. Diese Erfindung findet insbesondere Anwendung bei Chipkarten, da diese gegen Manipulationen von außen besonders gesichert sein müssen.
- 10 Es ist bekannt, Speicherbereiche eines Rechners zum Beispiel durch Busverschlüsselung, Speicherverschlüsselung und dergleichen gegen Manipulationen zu schützen. Aus DE 37 09 524 C2 ist beispielsweise eine Prüfroutine zur Überprüfung der Speicherzelleninhalte eines Programmspeichers bekannt.
- 15 Durch Prüfsummenbildung über die Speicherzelleninhalte jeweils zu Beginn oder während eines laufenden Programms und Vergleich mit einer im Programmspeicher zuvor abgelegten Prüfsumme läßt sich eine Veränderung der ursprünglichen Speicherzelleninhalte oder auch eine erst im Betrieb auftretende Veränderung erkennen, was zu einer Fehlermeldung führt.
- 20 Aufgabe der vorliegenden Erfindung ist es, eine Möglichkeit vorzuschlagen, wie der Rechner gegen äußere Manipulationen besser gesichert werden kann.
- 25 Die Aufgabe wird erfindungsgemäß durch ein Verfahren, durch eine zentrale Verarbeitungseinheit zur Durchführung dieses Verfahrens und durch einen Rechner bzw. eine Chipkarte mit einer solchen zentralen Verarbeitungseinheit gemäß den Merkmalen der nebengeordneten Ansprüche gelöst. In den Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung
- 30 angegeben.

Die Erfindung geht davon aus, daß durch eine Sicherung der im Rechnerkern, das heißt in der zentralen Verarbeitungseinheit (CPU) des Rechners, vorliegenden Daten gegen äußere Manipulationen die Sicherheit des Rechners erhöht werden kann, da im Rechnerkern die Daten unverschlüsselt vor-
5 liegen und daher leicht manipulierbar sind.

Um derartige Manipulation zu erkennen, wird nach der Verarbeitung eines Befehls durch die CPU aus mehreren Registerinhalten der CPU durch mathematische Verknüpfung, beispielsweise durch Exklusiv-Oder-
10 Verknüpfung (XOR-Verknüpfung), eine Checksumme ermittelt und als End-Checksumme in einem Speicher abgelegt. Vor der Verarbeitung des nächsten Befehls durch die CPU wird erneut eine Checksumme gebildet, das ist die Anfangs-Checksumme. Durch Vergleich der Anfangs-Checksumme mit der End-Checksumme, die übereinstimmen müssen, läßt sich feststellen, ob Re-
15 gisterinhalte der CPU nach der letzten Befehlsverarbeitung manipuliert wurden. Als Registerinhalte kommen die Inhalte jener Bereiche der CPU in Betracht, die einen von Null verschiedenen Zustand annehmen können, wie z.B. bei dem Prozessortyp 8051 der Accu, B-Accu, Datapointer (DPTR, DPL, DPH), Register (R0 bis R7) der Registerbänke, Programmstatuswort (PSW),
20 Stackpointer (SP), Special Function-Register (SPR) und dergleichen.

Zur weiteren Erhöhung der Sicherheit kann zusätzlich beim Laden eines Befehls ein Zähler gestartet werden, welcher die Taktzyklen, die zur Abarbeitung des Befehls notwendig sind, zählt. Der Zähler ist dabei vorzugsweise
25 hardwaremäßig aufgebaut. Eine Logik entnimmt dem Befehlsopcode die Anzahl der zur Abarbeitung notwendigen Taktzyklen und setzt diese in einen Zählerwert um. Der Zähler läuft dann parallel zum ausgeführten Befehl.

Es wird überprüft, ob der abzuarbeitende Befehl innerhalb der angegebenen Taktzyklen abgearbeitet wird. Für den Fall, daß der Befehl nicht innerhalb des vorgegebenen Zeitraums abgearbeitet wurde, wird beispielsweise die Taktversorgung eingestellt, so daß eine weitere Abarbeitung von Befehlen nicht mehr möglich ist. Alternativ kann auch ein Reset ausgelöst und somit die Zentraleinheit zurückgesetzt werden. Die gleichen Maßnahmen können getroffen werden, wenn der Befehl vorzeitig abgearbeitet wurde, d.h. wenn dem Befehlszähler noch nicht in seinem Grenzwert angelangt ist und bereits ein neuer Operationscode erkannt wurde.

10

Die logische Verknüpfung der sicherheitsrelevanten Register kann durch Hardware oder Software realisiert werden. Die Checksummenbildung zwischen zwei aufeinanderfolgenden Befehlen kann beispielsweise aufgrund zufälliger oder definierter Ereignisse oder ständig erfolgen.

15

Die Erfindung wird nachfolgend anhand der Zeichnungen näher erläutert.
Es zeigen:

Fig. 1 den Aufbau eines Mikrocontrollers am Beispiel eines 8051-Prozessors und

20

Fig. 2 eine Logik zur Verknüpfung mehrerer Bereiche der zentralen Verarbeitungseinheit.

Fig. 1 zeigt den Aufbau eines 8051-Prozessors, das ist ein 8-Bit-Prozessor. Während mit bekannten Verschlüsselungsverfahren die Daten durch Bus- oder Speicherverschlüsselung vor Manipulation geschützt werden, liegen die Daten im Kern des Rechners, d. h. in der zentralen Verarbeitungseinheit bzw. CPU, unverschlüsselt vor. Mit dem erfindungsgemäßen Verfahren

25

wird nun ermittelt, ob eines oder mehrere Register der CPU manipuliert worden sind.

- In Fig. 2 sind beispielhaft solche sicherheitsrelevanten Bereiche der CPU angegeben, die manipuliert werden könnten, nämlich Stackpointer SP, Akku AC, B-Akku BAC, Register RO bis R7, Data-Pointer DPL und DPH zu den unteren bzw. oberen Bereichen des internen RAM. Diese Register werden miteinander logisch verknüpft, um eine Checksumme zu bilden. In Fig. 2 sind jeweils zwei 8-Bit-Register durch ein Exklusiv-Oder-Gatter (XOR) miteinander verknüpft. So ergibt sich aus der XOR-Verknüpfung der Register RO und ein neues 8-Bit-Muster, das wiederum XOR-verknüpft wird mit dem 8-Bit-Muster, das sich aus der XOR-Verknüpfung der Register R1 und R7 ergibt. Durch weitere XOR-Verknüpfung der sich jeweils ergebenden 8-Bit-Muster ergibt sich schließlich ein 8-Bit-Muster, das als Checksumme dient und in Fig. 2 mit „Anfangs-Checksumme“ bezeichnet ist. Anstelle der XOR-Verknüpfung, welche insbesondere hinsichtlich des Aufwandes vorteilhaft ist, können selbstverständlich auch andere Ausführungsformen zur Bildung der Checksumme gewählt werden.
- 20 Wenn die Verknüpfung der Register hardwaremäßig durch logische Verknüpfungsglieder ausgeführt ist, ändert sich die Checksumme unmittelbar, wenn sich der Inhalt eines Registers ändert. D. h. , während der Abarbeitung eines in der CPU verarbeiteten Befehls ändert sich die Checksumme gegebenenfalls mehrfach. Entscheidend für die Durchführung des Verfahrens sind
- 25 aber nur die Checksumme nach Abarbeitung eines Befehls und vor Abarbeitung des nächstfolgenden Befehls, da diese beiden Checksummen (End-Checksumme des einen Befehls und Anfangs-Checksumme des nächstfolgenden Befehls) in einem Komparator miteinander verglichen werden.

Der Vergleich wird wie folgt durchgeführt: Die sich am Ende der Abarbeitung eines ersten Befehls einstellende Checksumme wird als End-Checksumme in einem Speicher auf der CPU abgelegt. Um nun festzustellen, ob nach der Abarbeitung dieses ersten Befehls und vor dem Laden des

5 nächstfolgenden, zweiten Befehls in die CPU eine Manipulation der CPU erfolgt ist, wird parallel zum Laden dieses zweiten Befehls die Anfangs-Checksumme wie eingangs beschrieben gebildet. In einem ersten Schritt a.) wird die Anfangs-Checksumme mit der in dem Speicher abgelegten End-Checksumme aus dem zuvor abgearbeiteten ersten Befehl mittels eines

10 Komparators verglichen. Für den Fall, daß keine Manipulation an der CPU vorgenommen worden ist, stimmen Anfangs- und End-Checksumme überein und der Wert des Vergleichsergebnisses ist Null. Der Komparator gibt ein Signal aus, aufgrund dessen in einem zweiten Schritt b.) nach Abarbeitung des zweiten Befehls die gerade anliegende Checksumme als neue End-

15 Checksumme in den Speicher eingespeichert wird. D. h. , die Abarbeitung des zweiten Befehls wird in diesem Falle nicht unterbrochen. Ergibt sich hingegen beim Vergleich der Anfangs-Checksumme mit der End-Checksumme ein Wert ungleich Null, so ist auf eine Manipulation der CPU zu schließen. Das Ausgangssignal des Komparators veranlaßt dann anstelle des zweiten

20 Schritts b.) eine Fehlermeldung c.), die in dem in Fig. 2 dargestellten Fall einen Abbruch der Befehlsverarbeitung verursacht. Beispielsweise kann der Prozessor angehalten werden, ein Sicherheitssensor kann aktiv geschaltet werden oder im Falle einer Chipkarte kann die Chipkarte vom Terminal ein-

behalten werden.

25

Der zuvor beschriebene Sicherheitsmechanismus kann auch rein softwaremäßig realisiert werden, indem die Checksummen einerseits am Ende einer Befehlsabarbeitung und andererseits zu Beginn der nächsten Befehlsabarbeitung ermittelt und miteinander verglichen werden. Das entsprechende Pro-

gramm kann beispielsweise in dem ROM bzw. EPROM des Prozessors gespeichert sein und die End-Checksumme kann in dem bitadressierbaren RAM des Prozessors abgelegt werden.

- 5 Das beschriebene Verfahren braucht nicht vor jedem abzuarbeitenden Befehl durchgeführt zu werden. Eine Ausgestaltung der Erfindung sieht vor, daß die Durchführung des Verfahrens von einem zufälligen oder einem definierten Ereignis abhängt. Gemäß einer ersten Ausführungsform kann das Verfahren zeitabhängig getriggert werden.

10

Gemäß einer anderen Ausführungsform kann das Verfahren dadurch getriggert werden, daß der Inhalt eines oder mehrerer Register der CPU einem vorbestimmten Muster entspricht.

- 15 Eine noch weitere Ausführungsform der Erfindung sieht vor, daß das Verfahren jeweils nach Verarbeitung einer vorgegebenen Anzahl von Befehlen getriggert wird.

- Bevorzugt wird eine Ausführungsform, wonach das Verfahren nur dann
20 getriggert wird, wenn zwischen dem Befehl, nach dessen Abarbeitung die Checksumme als End-Checksumme in den Speicher gespeichert wurde, und der Anfangs-Checksumme zu Beginn der Abarbeitung des nächstfolgenden Befehls eine längere, definierte Zeitspanne liegt. Dadurch wird wertvolle Rechnerkapazität bei der Ausführung eines Programms mit vielen Befehlen
25 gespart. Wenn man davon ausgeht, daß eine Manipulation der CPU, insbesondere bei Chipkarten, nicht während des laufenden Programms stattfindet, sondern wenn die Chipkarte aus dem Chipkartenterminal entfernt ist, so ist eine Manipulation der CPU mittels dieser zuletzt beschriebenen Ausführungsform dennoch zuverlässig feststellbar.

Patentansprüche

1. Verfahren zur Sicherung eines Rechners mit zentraler Verarbeitungseinheit (CPU) gegen äußere Manipulation, dadurch gekennzeichnet, daß anhand von sich am Ende der Verarbeitung eines Befehls durch die CPU einstellenden Registerinhalten der CPU durch mathematische Verknüpfung eine End-Checksumme gebildet und gespeichert wird und anhand der sich vor Beginn der Verarbeitung des nächstfolgenden Befehls durch die CPU einstellenden Registerinhalte eine Anfangs-Checksumme gebildet wird, wobei eine Fehlermeldung erfolgt, wenn die Anfangs-Checksumme nicht mit der End-Checksumme übereinstimmt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß beim Laden des Befehls ein Zähler gestartet wird, welcher die Taktzyklen, die zur Abarbeitung des Befehls notwendig sind, zählt und bei Über- oder Unterschreiten der vorgegebenen Taktzyklen ein Fehlersignal ausgibt.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß das Fehlersignal einen Interrupt auslöst oder zur Einstellung der Taktsignalversorgung führt.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Anzahl der zur Abarbeitung eines Befehls notwendigen Taktzyklen aus dem OP-Code des Befehls durch eine Logikschaltung erhalten wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die mathematische Verknüpfung mittels Exklusiv-Oder-Verknüpfung der Registerinhalte erfolgt.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Initiierung des Verfahrens durch zufällige oder definierte Ereignisse getriggert wird.

5 7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Verfahren zeitabhängig getriggert wird.

8. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Verfahren getriggert wird, wenn der Inhalt eines oder mehrerer Register der CPU ei-
10 nem vorbestimmten Muster entspricht.

9. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Verfahren jeweils nach Verarbeitung einer vorgegebenen Anzahl von Befehlen getrig-
15 gert wird.

10. Zentrale Verarbeitungseinheit (CPU) für einen Rechner zur Durchfüh-
rung des Verfahrens nach einem der Ansprüche 1 bis 6, umfassend

- eine Verknüpfung mehrerer Register der CPU durch logische Verknüp-
fungsglieder zur Bildung einer Checksumme,
- 20 - einen Checksummenspeicher zur Speicherung einer von den logischen
Verknüpfungsgliedern gebildeten, ersten Checksumme,
- einen Komparator zum Vergleichen einer von den logischen Verknüp-
fungsgliedern gebildeten, zweiten Checksumme mit der im Speicher ge-
speicherten, ersten Checksumme und
- 25 - eine Steuereinrichtung zum Steuern der Einspeicherung der ersten
Checksumme in den Checksummenspeicher und zum Steuern des Kom-
parators.

11. Zentrale Verarbeitungseinheit nach Anspruch 10, gekennzeichnet durch einen Zähler zum Zählen der für eine Befehlsabarbeitung benötigten Taktzyklen.
- 5 12. Zentrale Verarbeitungseinheit nach Anspruch 10 oder 11, gekennzeichnet durch eine Logikschaltung zum Bestimmen der für die Abarbeitung eines Befehls notwendigen Taktzyklen aus dem OP-Code des Befehls.
- 10 13. Rechner umfassend eine zentrale Verarbeitungseinheit nach einem der Ansprüche 10 bis 12.
14. Chipkarte umfassend eine zentrale Verarbeitungseinheit nach einem der Ansprüche 10 bis 12.



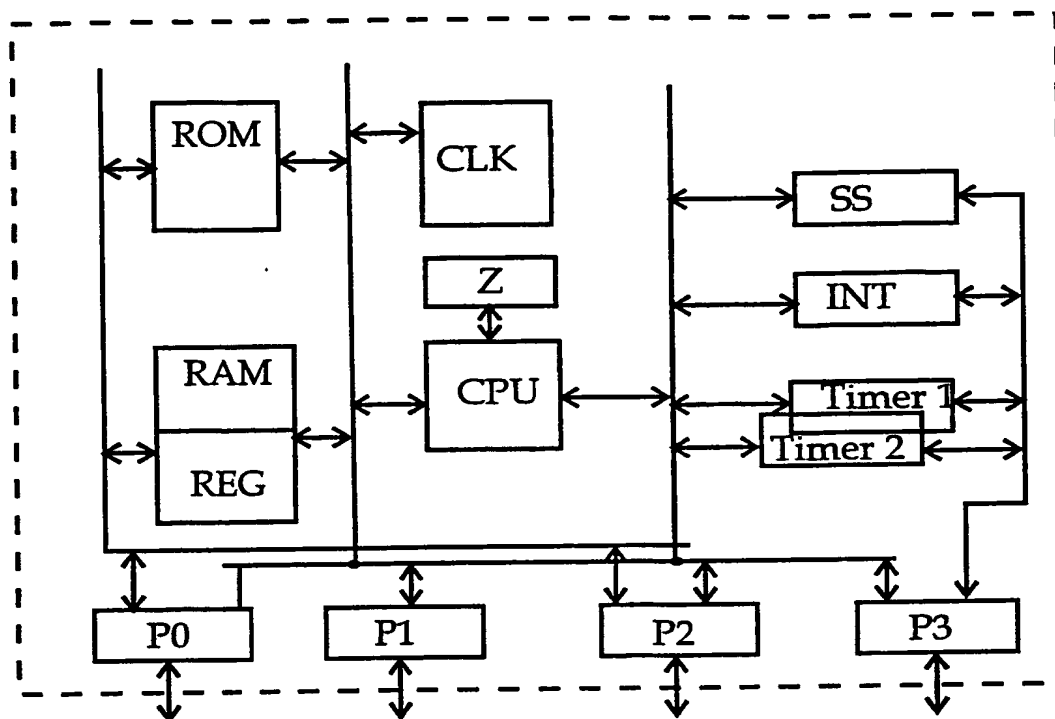


Fig. 1

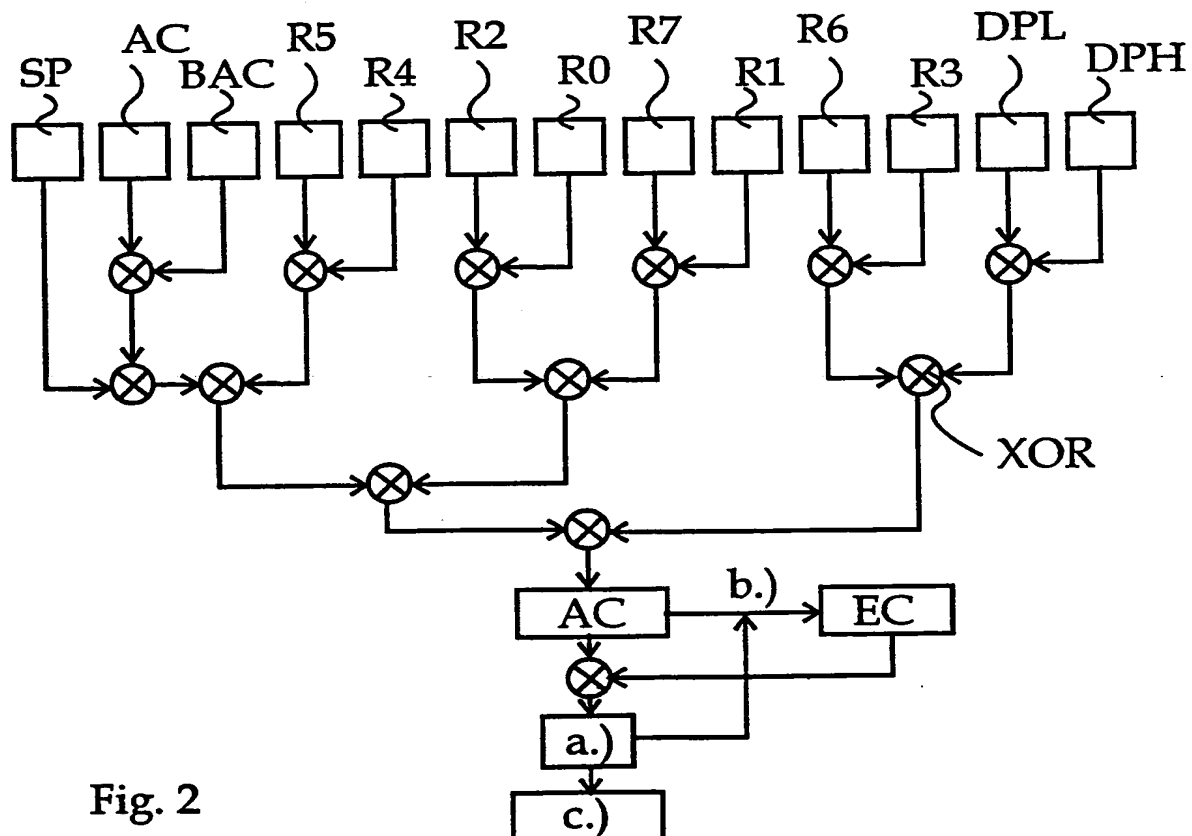


Fig. 2



1

2

3

4

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/03530

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

INSPEC, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 727 544 A (BRUNNER NORMAN ET AL) 23 February 1988 (1988-02-23) column 1, line 43 - line 62	1,10
A	WO 97 04394 A (DRAKE CHRISTOPHER NATHAN) 6 February 1997 (1997-02-06) page 7, line 28 - line 30; claim 9	2,11
A	RADAI Y: "CHECKSUMMING TECHNIQUES FOR ANTI-VIRAL PURPOSES" VIRUS BULLETIN CONFERENCE, GB, VIRUS BULLETIN LTD., ABINGTON, September 1991 (1991-09), pages 39-68, XP000700179 page 44, line 46 -page 45, line 5	5

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

17 August 2000

Date of mailing of the international search report

24/08/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fernandez Balseiro, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/03530

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4727544 A	23-02-1988	NONE	
WO 9704394 A	06-02-1997	AU 5945796 A US 6006328 A	23-01-1997 21-12-1999

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F11/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

INSPEC, EP0-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 4 727 544 A (BRUNNER NORMAN ET AL) 23. Februar 1988 (1988-02-23) Spalte 1, Zeile 43 - Zeile 62	1,10
A	WO 97 04394 A (DRAKE CHRISTOPHER NATHAN) 6. Februar 1997 (1997-02-06) Seite 7, Zeile 28 - Zeile 30; Anspruch 9	2,11
A	RADAI Y: "CHECKSUMMING TECHNIQUES FOR ANTI-VIRAL PURPOSES" VIRUS BULLETIN CONFERENCE, GB, VIRUS BULLETIN LTD., ABINGTON, September 1991 (1991-09), Seiten 39-68, XP000700179 Seite 44, Zeile 46 -Seite 45, Zeile 5	5



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

a Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

17. August 2000

Abschließdatum des internationalen Recherchenberichts

24/08/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Fernandez Balseiro, J

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 00/03530

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 4727544 A	23-02-1988	KEINE	
WO 9704394 A	06-02-1997	AU 5945796 A	23-01-1997
		US 6006328 A	21-12-1999